ANALYSIS OF VARIOUS MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR NETWORK INTRUSION DETECTION SYSTEM

[1]Punyashree B, [2]Radhika K R

[1]Student, [2] Professor
Department of Information Science and Engineering,
BMS College of Engineering, Bangalore, India

***Abstract*- A wide range of cyber-attacks have been happening on daily basis. Computers are always protected against the attacks but detecting intrusion in network is always helpful in preventing attacks and protecting the system. This paper provides a comprehensive analysis of machine learning and deep learning approaches used in Network Intrusion Detection Systems (NIDS). It explores the fundamental concepts and challenges of NIDS and highlights the limitations of traditional rule-based methods. Implementing the models and analyzing which is best accepted.**

***Index Terms*- intrusion detection, cyber-attacks, deep learning, network intrusion, machine learning.**

I. INTRODUCTION

Data security is now the most crucial responsibility because data is the most precious thing anyone may own. One example area where it offers data security is cyber security. Cyberattacks come in many forms, including phishing, the dissemination of false information on social media, cyberbullying, cyberstalking, and others. These attacks can be recognized and avoided in several ways. Network intrusion is one such assault; a tool or piece of software that watches a system for malicious behavior. In a network, it also finds harmful activity. If such activity is discovered, a centrally controlled system is notified. Intrusion detection takes the main role in addressing who intruded the system. There is major three types [1] of intrusion detection Intrusion detection based on "Network", "Host", "Application". Intrusion detection in "Network" is a framework for examining impending organized activity. These systems, installed at various points throughout the network, monitor all activity from all devices within the organization. They investigate activity passing on the subnet and attempt to match it with many of the known attacks. If an attack is identified or any unusual behavior is identified, a warning will be sent to the administrator. In order to detect any potential attempts to breach the firewall, these frameworks will be installed in subnets where firewalls are present. To improve the rate of detection and prediction, NIDS can also be used in conjunction with other technologies.

Intrusion detection based on "Host" keeps track on the computer infrastructure on which it is placed, analyzing traffic, and reporting hostile activity. You have extensive visibility into what's happening on your vital security systems thanks to a HIDS. It enables you to recognize suspicious or unusual activity in your environment and take appropriate action. Host intrusion detection cannot completely describe on its own the security posture. Your HIDS log data must be able to be correlated with other crucial security data as well as with the most recent real-world threat information.

Intrusion detection Based on "Application" is where the application is major focus, however occasionally, even if such a scenario is not present, the intrusion may have occurred while the application was operating. This is classified as host based. Conventional rule-based IDS are inefficient at spotting novel and developing assaults. The ability of machine learning (ML) and deep learning (DL) approaches to learn from data and recognize complicated patterns has led to their emergence as effective tools for network intrusion detection. Denial-of-service (DoS) assaults, port scans, and buffer overflow attacks have all been identified by ML and DL-based (NIDS). The ability to evaluate massive volumes of data and spot small trends that could point to malicious behavior is the main benefit of utilizing ML and DL approaches for NIDS. Conventional rule-based approaches, which rely on predetermined criteria to identify assaults, have a limited capacity to recognize new and developing threats.

NETWORK INTRUSION PREVENTION SYSTEM:

An example of security technology used to keep an eye on network activity and stop illegal access to computer systems is the Network Intrusion Prevention System (NIPS). It operates by scrutinizing incoming communications and contrasting it with a database of recognized risks and attack patterns. To find and stop network intrusions, NIPS employs several methods, such as signature-based detection, behavior-based detection, and anomaly detection. The system can automatically restrict traffic or take other preventative measures when an intrusion is discovered to stop the attack from being successful. As it may assist enterprises in defending against a variety of threats, such as malware, viruses, and other forms of cyberattacks, NIPS is a important part of network security. Potential risks are discovered by keeping an eye on network traffic.

TYPES OF NIDS:

Network Intrusion detection are of 2 types which are Signature and anomaly based. A key component of cybersecurity that aids in shielding enterprises from harmful attackers is network intrusion detection. Network intrusion detection techniques such as

signature-based intrusion detection look for patterns of malicious and suspicious activity in network traffic and flag any traffic that resembles known attack signatures. Because it looks for the distinguishing characteristics of different assaults, this type of IDS can identify malicious activity with a high degree of accuracy. Moreover, signature-based IDS can be used to spot well-known attack patterns like buffer overflows and SQL injections as they detect unusual network activity it can be an attack sign. Organizations may stay one step ahead by using signature-based intrusion detection to monitor for malicious activities and identify questionable traffic. An approach to NIDS known as anomaly-based intrusion detection detects departures from typical or anticipated network activities. This IDS monitors network traffic and looks for any intrusions that might point to malicious activity using machine learning methods. Anomaly based intrusion detecting is more dynamic and can identify novel or previously unidentified attack patterns than signature-based intrusion detection, which depends on pre-defined attack signatures to identify malicious behavior. An organization's network can be utilized to identify insider threats and malicious activity using anomaly-based IDS. Anomaly-based intrusion detection can assist organizations in identifying and responding to possible security threats before they become a significant problem by monitoring network traffic and detecting any irregularities.

II. LITERATURE REVIEW

[1] Attacks on a computer network can be discovered using an intrusion detection system (IDS). Using the KDDCup99 Test datasets, machine learning techniques such Bayes Net, Random Forest, and Random Tree were examined for the classification of these attacks into their many classifications. With the Best First search approach and parameters like Precision, Recall, and F-measure being computed for feature selecting on the dataset, WEKA was utilized as the experimental tool. The results demonstrated that the most accurate classification of data sets was by the Random Forest and Random Tree algorithms.[2] As a result of technological innovation, more people are using the Internet and its various connected devices. This larger network complicates things and gives attackers more room to investigate and find flaws to employ in a variety of assaults. Finally, the result there is a recent increase in network attacks that are diverse, as evidenced by the admission of different companies. To address these difficulties, many intrusion detection systems (IDSs) have been developed and put out that use misuse-based, anomaly-based, and occasionally mixed methodologies. It is difficult for IDSs to maintain their efficacy and dependability due to the increasing rate of network data production and its vast volume.[3] This research uses ML algorithms to provide an ensemble strategy for intrusion detection systems (IDS). The authors talk about the value of IDS in the modern world and how it may be used to identify hostile activity on a computer network by integrating various machine learning algorithms and approaches, such as supervised or unsupervised categorization methods. Also, they discuss the importance of feature selection while designing these systems as well as several methods that could be used, such as Information Gain or Bootstrapping. Also, they describe their results, which demonstrate that Ensemble Approach outperforms other classifiers in terms of precision, recall, and accuracy metrics while drastically lowering total count of features needed for detection tasks when comparing to conventional models. Lastly, they offer suggestions for additional advancements required to construct more effective IDS systems that can accurately identify all types of threats without sacrificing security requirements outlined by enterprises around the world.[4] Machine learning models have been used as the major strategies in this research to identify malicious attacks. The Knowledge Discovery in Databases (KDD) dataset, which contains 21 types of assaults including DOS, R2L, U2R, and PROBE, has been used to evaluate these classifiers. For testing, 60000 instances from the KDD dataset were taken, with all 21 forms of attacks represented. • The efficacy of these models at detecting intrusions was assessed using performance criteria such as false negative and false positive rate.[5] The article describes an experimental investigation of a machine learning-based prototype intrusion detection system in mobile ad hoc networks. The experiment is run in a MANET segment with 50 nodes, and it investigates DDoS and cooperative blackhole attack detection and prevention. It is explored how features depend on the type of network traffic and how performance metrics depend on how quickly mobile nodes move around the network. The outcomes of the carried out experimental investigations demonstrate the efficacy of a prototype IDS using simulated data.

[6] In this article, we proposed a machine learning-based methodology to identify network intrusions. Preprocessing, feature selection, parameter optimization, and classification are the four primary stages of the suggested methodology. The Feature Selection is based on correlation is used to choose the most important attributes. Particle swarm optimization is utilized for parameter optimization while Random Tree, AdaBoost, K-Nearest Neighbor (KNN), and Support-vector machine (SVM) are used for classification. The new technique was examined using the NSL-KDD and CIC-DDOS2019 large datasets. The experimental results show that the suggested method outperforms the other machine learning techniques and can efficiently categorize intrusions with a high detection rate.[7] An IDS should be able to tell the difference between a genuine packet and an invader by observing their behavior. The suggested system uses neural networks and support vector machine (SVM) models for detection of intrusion to stop security risks in a local area network (LAN). The KDD99 dataset is used to test the suggested approach. A benchmark for anomaly-based detection is the KDD99. This method efficiently and quickly detects attacks. It is done to check and compare the effectiveness of the SVM and neural network models. According to findings, neural networks outperformed all SVM kernel models in terms of classification accuracy. The SVM linear kernel performs significantly best than the SVM polynomial kernel and slightly better than the SVM gaussian kernel.

[8] In this study, machine and deep learning techniques for intrusion detection systems are analyzed. The study makes use of the CICIDS2017 dataset, which has 79 features. The algorithms of random forests and multilayer perceptron (MLPs) are used. Information gain, extra trees, random forests, and correlation are four features extraction strategies that are taken into consideration for experimentation. The first model uses the deep learning multilayer perceptron (MLP) technique, and the second uses the machine learning's random forest (RF) approach. The use of the random forest method has been shown to boost accuracy. The four feature selection strategies perform best when using the RF algorithm, demonstrating that RF is superior to MLP.[9] The author suggests a deep learning-based approach to NIDS. This technique uses BP neural networks as top-level classifiers for the classification of intrusion types and Deep Confidence Neural Networks to extract features from network monitoring data. It was examined using

the KDD CUP'99 dataset from the Massachusetts Institute of Technology's Lincoln Laboratory (MIT). The outcomes demonstrate that the accuracy of the proposed methods is significantly higher than that of conventional machine learning.[10] The primary strategy covered in this study is the utilization of deep learning architectures to create a flexible and dependable network intrusion detection system (IDS). • This IDS can quickly remove intruders from systems thanks to its capacity to detect both known and undiscovered behavioral aspects. The UNSW-NB15 dataset, which reflects actual contemporary communication behavior with synthetically generated attack actions, is utilized to show the system's efficacy.[11] This work proposes an end-to-end model for network attack detection and network attack classification using deep learning-based recurrent models. The proposed model extracts the features of hidden layers of recurrent models and further employs a kernel-based principal component analysis (KPCA) feature selection approach to identify optimal features. Finally, the optimal features of recurrent models are fused together, and classification is done using an ensemble meta-classifier. Experimental analysis and results of the proposed method on more than one benchmark network intrusion dataset show that the proposed method performed better than the existing methods and other most used machine learning and deep learning models. In particular, the proposed method showed maximum accuracy 99% in network attacks detection and 97% network attacks classification using the SDN-IoT dataset. Similar performances were obtained by the proposed model on other network intrusion datasets such as KDD-Cup-1999, UNSW-NB15, WSN-DS, and CICIDS-2017.[12] By evaluating the literature and providing background information on either deep learning or machine learning algorithms on intrusion detection systems, the major goal of this study is to survey in-depth learning and machine learning models for intrusion detection. Using the DARPA dataset, the paper also compares the effectiveness of various machine learning categorization techniques.
[13] NSL-KDD training and validation data, which is widely used in intrusion detection, was utilized to calculate, and compare the accuracy, precision, and recall comparing the detection results of the two approaches. The accuracy of the DNN model is higher than that of the SVM model. DNN outperforms SVM in terms of intrusion detection because it is far riskier to mistake normal data for an intrusion than it is to mistake normal data for an incursion.[14] detection of multiple network breaches, including attacks from the User to Root, the Remote to User, and the Denial of Service (U2R). PSO-SVM, RBF, and C means clustering algorithms have been used in a performance analysis and comparison study. This study proposes the new serial and parallel IDS model.[15] For enhancing the performance of the intrusion detection system, combined model of machine larning which consists of supervised and unsupervised learning models is presented, along with feature selection method. Experiments on the NSL KDD dataset showed that the accuracy level of our proposed model was 11% greater than that of other approaches such as AdaBoost, XG Boost, Random Forest, Gaussian Naive Bayes, and LGB.[16] Deep learning technology is being employed more and more in the realm of security, and the text's intrusion detection classification model is built using a deep learning classification network. The original intrusion data is processed before using the right data processing technology, and the processed data is then used to train the network model. Lastly, the model's effectiveness is evaluated to attain high classification accuracy.[17] Researchers have addressed the input-hidden layer's erratic weights as a problem with NID. As a result, both the convergence and the speed are of importance. For combining NID with Long Short-Term Memory, it describes the NID-Recurrent Neural Network (RNN) technique (LSTM). The method is tested utilizing various activation function situations for NID on the one hand, and the quantity of iterations for BP on the other. The performance of the suggested model based on binary and multiclass classifications is assessed using the UNSW-NB18 datasets. The experimental findings demonstrate that, in order to get the best accuracy with a minimal amount of iterations, the accuracy of the suggested RNN was raised by roughly 8% when compared to the existing RNN technique.[18]Most have used machine learning algorithms for NID's but here author used deep neural networks for network data and the same is validated using KDDcup99 dataset and NSL-KDD dataset. Deep neural network is the major model [19] for creating an effective network intrusion detection system which even detect and classify unforeseen cyberattacks. There are many other deep learning techniques for intrusion detection as [20] the author in order to get better performance, the suggested model was trained utilizing the mini-batch gradient descent technique, L1 regularization technique, and ReLU activation function. Findings using the KDDCUP'99 dataset demonstrate that our method outperforms previous deep sparse autoencoder network intrusion detection systems in terms of performance.

Based on Dataset	**Methodology – which authors have worked on**	**Advantage**	**Limitation**
KDDcup99 [3]	Naive Bayes, Adaptive Boost, Partial Decision tree, Neural Network, Support Vector Machine (SVM)	Both ML and DL algorithms have been used	Only few algorithms have been used.
NSL-KDD (Improvements on KDDcup99) [3]	AdaBoost, XG Boost, Random Forest, Gaussian Naive Bayes, LGB, SVM, DNN, Random Tree, AdaBoost, K-Nearest Neighbor (KNN)	Dataset is used for most of the ML and DL models.	Different authors used different algorithms comparison isn't proper.

CICIDS2017[2]	Random forest (RF), Multilayer perceptron (MLP), RNN, LSTM, and GRU	Most of the algorithms are of deep learning	As only Deep learning is used can't be a comparative study

Table 1: Anomaly based dataset comparison Table along with the methodology used.

III. METHODOLOGY

A. Description

A dataset including a wide range of simulated incursions into a military network environment was made available for assessment. By emulating a typical US Air Force LAN, it established a setting for acquiring raw TCP/IP dump data for a network. The LAN was bombarded with several attacks and concentrated like a genuine atmosphere. A connection is a series of TCP packets that begin and stop at specific times and allow data to flow from a source IP address to a target IP address according to a specific protocol. Additionally, each link has a label designating it as either normal or an attack of exactly one particular attack kind. An average connection record is 100 bytes long.

From normal and attack data, 41 quantitative and qualitative features (3 qualitative and 38 quantitative features) are gleaned for each TCP/IP connection.

Two categories make up the class variable:

• Regular

• Abnormal

There is two set of data one is for testing, and one is for training.

The Train dataset contains 25192 records of data and test dataset contains 22544 records.

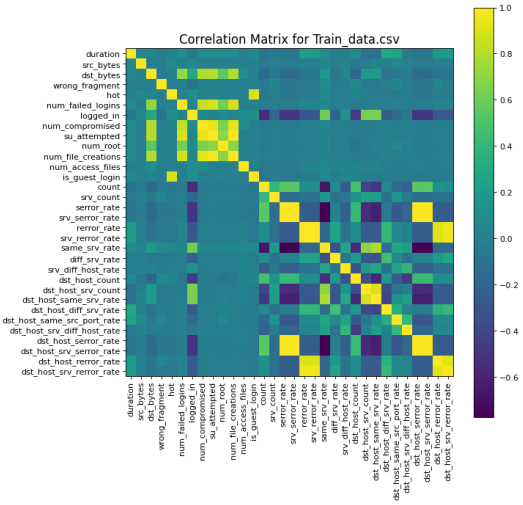

Figure 1: Correlation Matrix diagram for Train dataset.

The above picture shows the correlation matrix for training data set correlation matrix suggest to see the missing data the correlation matrix is basically used to map between the variables to know how they are correlated , by this we can know the missing data and we can encode the values as well here the picture shows the correlation of training data set is a correlation of the coefficient of the variables.

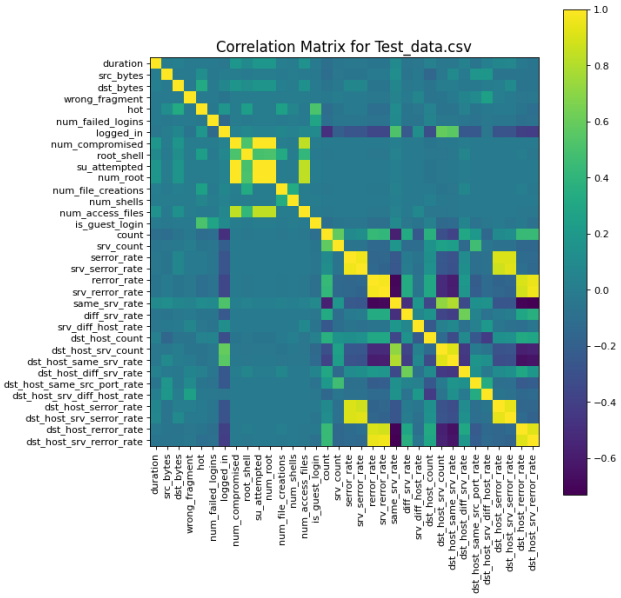

Figure 2: Correlation Matrix diagram for Test dataset.

The correlation matrix for test dataset the correlation matrix in the above diagram shows the correlation between the attributes of the data set where it is chosen only Android rose to limit it because the data set of test data set has more than 22,000 data.

Data profiling to know what the columns are available to check the null values present and to remove if any because the null values doesn't consider when feeding into the models.

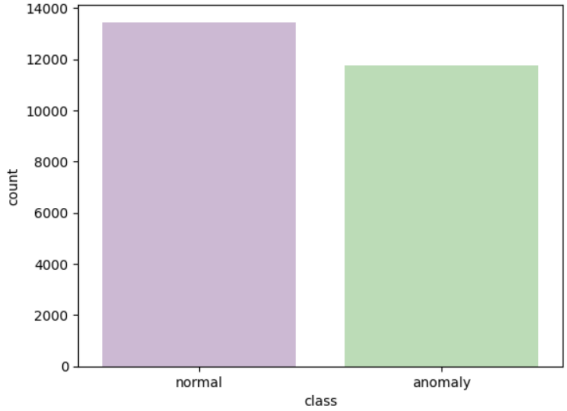

Figure 3: Bar graph for train data for normal and anomaly classification.

The above diagram shows the difference between normal data and anomaly data present in training data set this graph is obtained after profiling and preprocessing the data to know what the ratio is of normal and anomaly.

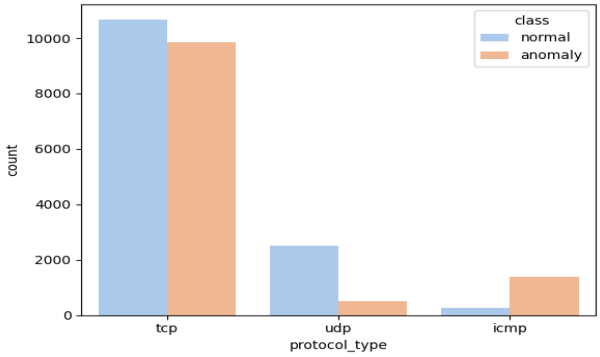

Figure 4: Bar graph for train data for different protocols.

The above diagram shows the TCP layer UDP layer and ICMP layer data corresponding to normal and anomaly classification this is to show even TCP IP and UDP and ICMP , here are present in the data set taken.

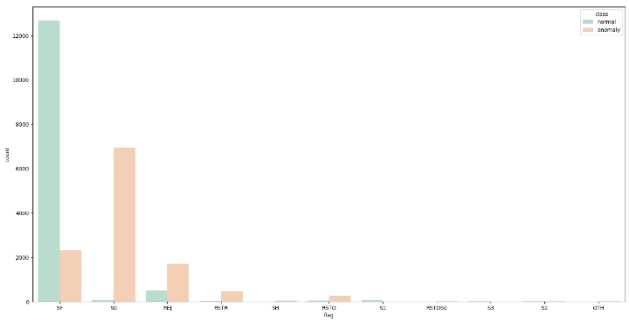

Figure 5: Bar graph for train data for different features for anomaly and normal data.

In this diagram it is showing for each label how the normal and anomaly classification has been distributed like for example if you see for the first label the normal is more an anomaly is less and for the second one the normal is very less and anomaly is huge so this shows which features should be taken while considering into model

A. Data preprocessing

while training the data the preprocessing is required encoding the values using label encoder.
Encoding is also and very important step as when we have null values or when we have mismatched data to maintain it properly, we need to encode the data.

Feature selection part is very important as there will be many labels, but we can't feed all the labels into the model, so we'll be taking only few labels or features which are very important in the sense which have maximum values, and which doesn't have most null values to get the maximum result.

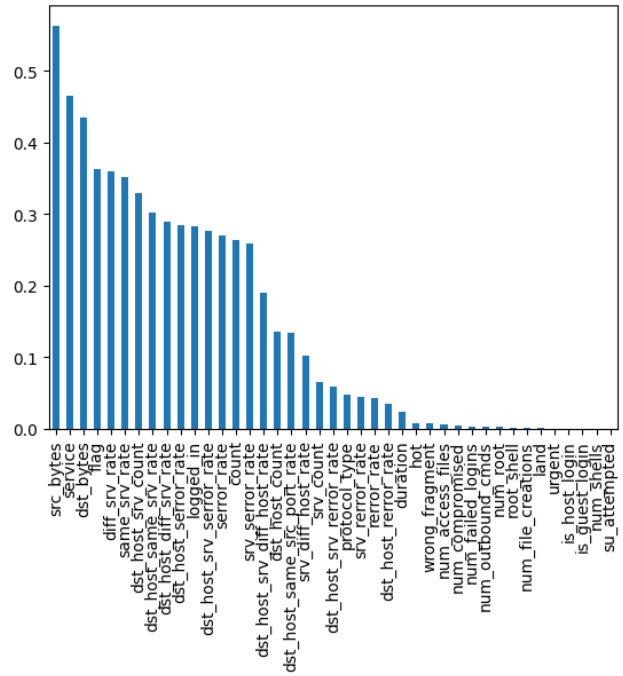

Figure 6: Bar graph for train data for feature selecting.

B. Data Splitting

The above graph shows the crux features using the bar graph. The important feature here is the source bytes, constitute considering the echo image will be taking 15 as important features for the model. Once the features are selected now the data will be split.

C. Machine learning and Deep Learning Algorithms

Computer algorithms known as "machine learning algorithms" allow computers or other devices to recognize patterns and come to conclusions or predictions without having to be explicitly programmed. These techniques enable systems to recognize patterns in data, learn from it, and enhance their performance over time.
Data is already labeled the models considered here are only classification models the four models which I am considering for analyzing is:

- Random Forest Classifier
- XGB classifier
- Bagging classifier
- Adaboost classifier

these are the four machine learning models I have chosen and one more model from deep learning i.e.,
"Artificial neural network".
Random Forest is an ensemble method that makes predictions by combining various decision trees. It is renowned for being reliable and capable of handling complicated datasets. Extreme Gradient Boosting, or XG Boost, is a well-liked machine learning technique that is frequently used for both regression and classification applications. It is sophisticated application of gradient boosting that has attracted more interest and excelled in a number of machine learning contests. Bagging, also known as bootstrap aggregating, is a machine learning ensemble strategy that combines many models that have been trained using various subsets of the training data to increase the precision and stability of predictions. Most of its applications are in classification and regression tasks. The machine learning ensemble technique AdaBoost (Adaptive Boosting) combines weak learners (usually decision trees) to produce a powerful predictive model. It works well for binary classification jobs but may also be applied to regression issues. A computational model called an artificial neural network (ANN), commonly referred to as a neural network, is one that is motivated by the composition and operation of the human brain. It is a potent machine learning method that is utilized for many different tasks like pattern recognition, classification, regression, and optimization.
As this is ensemble approach taken five models to analyze and compare. For the ANN approach 15 has been selected build sequentially using keras classifier.

IV. RESULTS AND DISCUSSION

Algorithm	Accuracy
Random Forest Classifier	99.77%
bagging classifier	99.77%
XGB classifier	99.60%
Ada boost classifier	98.82%
Artificial neural networks	97.86%

Table 2: Algorithm vs their Accuracy score

the table has the accuracy score for random forest classifier is 1 which is very high as it was a labeled data the classifier algorithms give better results and neural networks got 97% among all the classifiers. For both machine learning algorithms and even neural network are hard had only 15 features to make it comparatively easy to understand, the results of accuracy have been taken.
Comparative analysis for machine learning programs regarding train and test data. Accuracy, recall, precision and f1 score as being given in the below table.

	Train_Accuracy Score	Train_Precision Score	Train_F1Score	Train_Recall	Test_Accuracy Score	Test_Precision Score	Test_F1Score	Test_Recall	Test_AUC_Score
RandomForestClassifier	1.00000	1.000000	1.000000	1.00000	0.997751	0.997528	0.997898	0.997751	0.997712
BaggingClassifier	1.00000	1.000000	1.000000	1.00000	0.997221	0.997033	0.997403	0.997221	0.997180
XGBClassifier	0.99983	0.999894	0.999841	0.99983	0.996031	0.997027	0.996286	0.996031	0.996067
AdaBoostClassifier	0.98588	0.982711	0.986821	0.98588	0.988224	0.985507	0.989030	0.988224	0.987899

Table 2 : Accuracy score for machine learning algorithms.

Confusion matrix for ANN model is given below and even the test for ANN confusion matters has been added.

```
============================== ANN Model Evaluation ====================

Cross Validation Mean Score:
 0.9791314601898193

Model Accuracy:
 0.9828739934217988

Confusion matrix:
 [[7978  267]
 [  35 9354]]

Classification report:
              precision    recall  f1-score   support

           0       1.00      0.97      0.98      8245
           1       0.97      1.00      0.98      9389

    accuracy                           0.98     17634
   macro avg       0.98      0.98      0.98     17634
weighted avg       0.98      0.98      0.98     17634
```

Figure 6: This represents the confusion matrix and accuracy score for model evaluation for ANN.

```
============================== ANN Model Test Results ==========

Model Accuracy:
 0.9786980682720297

Confusion matrix:
 [[3365  133]
 [  28 4032]]

Classification report:
              precision    recall  f1-score   support

           0       0.99      0.96      0.98      3498
           1       0.97      0.99      0.98      4060

    accuracy                           0.98      7558
   macro avg       0.98      0.98      0.98      7558
weighted avg       0.98      0.98      0.98      7558
```

Figure 7: This represents the confusion matrix and accuracy score for model evaluation for ANN.

IV. CONCLUSION

The research and implementation helpful in understanding the intrusion detection system for anomaly based. the random forest classifier end bagging classifier has classified the data oh test accuracy is 99% both the classifier has given the maximum result even in training accuracy as well as test accuracy. while considering artificial neural network as given 97% accuracy score but took lot of serials to get it which is very time consuming. Hence by observing the implementation under research shows random forest and bagging classifier can be used for labeled anomaly-based network intrusion data.

REFERENCES:

1. Ugochukwu, C. J., & Bennett, E. O. (n.d.). "*An intrusion detection system using machine learning algorithm*". Iiardjournals.org. Retrieved February 22, 2023, from https://www.iiardjournals.org/get/IJCSMT/VOL.%204%20NO.%201%202018/An%20Intrusion%20Detection.pdf
2. Keserwani, P. K., Govil, M. C., & Pilli, E. S. (2021). "*An effective NIDS framework based on a comprehensive survey of feature optimization and classification techniques"*. In Neural Computing and Applications (Vol. 35, Issue 7, pp. 4993–5013). Springer Science and Business Media LLC. https://doi.org/10.1007/s00521-021-06093-5
3. Kumar Singh Gautam, R., & Doegar, Er. A. (2018). "*An Ensemble Approach for Intrusion Detection System Using Machine Learning Algorithms"*. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE. https://doi.org/10.1109/confluence.2018.8442693
4. Chalé, M., & Bastian, N. D. (2022). "*Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems"*. In Expert Systems with Applications (Vol. 207, p. 117936). Elsevier BV. https://doi.org/10.1016/j.eswa.2022.117936
5. Legashev, L., & Grishina, L. (2022). "*Development of an Intrusion Detection System Prototype in Mobile Ad Hoc Networks Based on Machine Learning Methods"*. In 2022 International Russian Automation Conference (RusAutoCon). 2022 International Russian Automation Conference (RusAutoCon). IEEE. https://doi.org/10.1109/rusautocon54946.2022.9896238
6. Yilmaz, A. A. (2022). "*Intrusion Detection in Computer Networks using Optimized Machine Learning Algorithms"*. 2022 3rd International Informatics and Software Engineering Conference (IISEC). https://doi.org/10.1109/iisec56263.2022.9998258
7. Aljohani, A., & Bushnag, A. (2021). "*An Intrusion Detection System Model in a Local Area Network using Different Machine Learning Classifiers"*. In 2021 11th International Conference on Advanced Computer Information Technologies (ACIT). 2021 11th International Conference on Advanced Computer Information Technologies (ACIT). IEEE. https://doi.org/10.1109/acit52158.2021.9548421
8. Hagar, A. A., & Gawali, B. W. (2022). "*Implementation of Machine and Deep Learning Algorithms for Intrusion Detection System"*. In Intelligent Communication Technologies and Virtual Mobile Networks (pp. 1–20). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-1844-5_1
9. Peng, W., Kong, X., Peng, G., Li, X., & Wang, Z. (2019). "*Network Intrusion Detection Based on Deep Learning"*. In 2019 International Conference on Communications, Information System and Computer Engineering (CISCE). 2019 International Conference on Communications, Information System and Computer Engineering (CISCE). IEEE. https://doi.org/10.1109/cisce.2019.00102
10. Ashiku, L., & Dagli, C. (2021). "*Network Intrusion Detection System using Deep Learning"*. In Procedia Computer Science (Vol. 185, pp. 239–247). Elsevier BV. https://doi.org/10.1016/j.procs.2021.05.025
11. Ravi, V., Chaganti, R., & Alazab, M. (2022). "*Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system"*. In Computers and Electrical Engineering (Vol. 102, p. 108156). Elsevier BV. https://doi.org/10.1016/j.compeleceng.2022.108156
12. Abraham, J. A., & Bindu, V. R. (2021). "*Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review"*. In 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). 2021 International Conference on Advancements in Electrical,

Electronics, Communication, Computing and Automation (ICAECA). IEEE. https://doi.org/10.1109/icaeca52838.2021.9675595

13. Patel, N. D., Mehtre, B. M., & Wankar, R. (2022). "*Detection of Intrusions using Support Vector Machines and Deep Neural Networks"*. In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE. https://doi.org/10.1109/icrito56286.2022.9964756
14. Das, I., Singh, S., & Sarkar, A. (2021). "*Serial and Parallel based Intrusion Detection System using Machine Learning"*. In 2021 Devices for Integrated Circuit (DevIC). 2021 Devices for Integrated Circuit (DevIC). IEEE. https://doi.org/10.1109/devic50843.2021.9455936
15. Mashuqur Rahman Mazumder, A. K. M., Mohammed Kamruzzaman, N., Akter, N., Arbe, N., & Rahman, M. M. (2021). "*Network Intrusion Detection Using Hybrid Machine Learning Model"*.In 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). IEEE. https://doi.org/10.1109/icaect49130.2021.9392483
16. Huang, X., Li, Y., Ou, L., Shu, F., & Ma, W. (2022). "*Research and Implementation of Industrial Control Network Security Intrusion Detection Classification based on Deep Learning"*. In 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). IEEE. https://doi.org/10.1109/itaic54216.2022.9836915
17. S. Amutha, K. R, S. R and K. M, "*Secure network intrusion detection system using NID-RNN based Deep Learning*", 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752526
18. Hussain, J., & Hnamte, V. (2021). "*Deep Learning Based Intrusion Detection System: Modern Approach"*. In 2021 2nd Global Conference for Advancement in Technology (GCAT). 2021 2nd Global Conference for Advancement in Technology (GCAT). IEEE. https://doi.org/10.1109/gcat52182.2021.9587719
19. Navya, V. K., Adithi, J., Rudrawal, D., Tailor, H., & James, N. (2021). "*Intrusion Detection System using Deep Neural Networks (DNN)"*. In 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). IEEE. https://doi.org/10.1109/icaeca52838.2021.9675513
20. Tanimu, J. J., Hamada, M., Robert, P., & Mahendran, A. (2022). "*Network Intrusion Detection System Using Deep Learning Method with KDD Cup'99 Dataset"*. In 2022 IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC). 2022 IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC). IEEE. https://doi.org/10.1109/mcsoc57363.2022.00047
21. Pontes, C. F. T., de Souza, M. M. C., Gondim, J. J. C., Bishop, M., & Marotta, M. A. (2021). "*A New Method for Flow-Based Network Intrusion Detection Using the Inverse Potts Model"*. In IEEE Transactions on Network and Service Management (Vol. 18, Issue 2, pp. 1125–1136). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/tnsm.2021.3075503
22. Duan, G., Lv, H., Wang, H., & Feng, G. (2023). "*Application of a Dynamic Line Graph Neural Network for Intrusion Detection With Semisupervised Learning"*. In IEEE Transactions on Information Forensics and Security (Vol. 18, pp. 699–714). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/tifs.2022.3228493